

1. A technician notices that an application is not responding to commands and that the computer seems to respond slowly when applications are opened. What is the best administrative tool to force the release of system resources from the unresponsive application?

- **Task Manager**
- Event Viewer
- System Restore
- Add or Remove Programs

Explanation: Use the Task Manager **Performance** tab to see a visual representation of CPU and RAM utilization. This is helpful in determining if more memory is needed. Use the **Applications** tab to halt an application that is not responding.

2. Which two commands could be used to check if DNS name resolution is working properly on a Windows PC? (Choose two.)

- **nslookup cisco.com**
- net cisco.com
- nbtstat cisco.com
- ipconfig /flushdns
- **ping cisco.com**

Explanation: The **ping** command tests the connection between two hosts. When **ping** uses a host domain name to test the connection, the resolver on the PC will first perform the name resolution to query the DNS server for the IP address of the host. If the ping command is unable to resolve the domain name to an IP address, an error will result.

Nslookup is a tool for testing and troubleshooting DNS servers.

3. A technician has installed a third party utility that is used to manage a Windows 7 computer. However, the utility does not automatically start whenever the computer is started. What can the technician do to resolve this problem?

- Uninstall the program and then choose Add New Programs in the Add or Remove Programs utility to install the application.
- Set the application registry key value to one.

- **Change the startup type for the utility to Automatic in Services.**
- Use the Add or Remove Programs utility to set program access and defaults.

Explanation: The Services console in Windows OS allows for the management of all the services on the local and remote computers. The setting of Automatic in the Services console enables the chosen service to start when the computer is started.

4. A PC user issues the netstat command without any options. What is displayed as the result of this command?

- a historical list of successful pings that have been sent
- a local routing table
- **a list of all established active TCP connections**
- a network connection and usage report

Explanation: When used by itself (without any options), the netstat command will display all the active TCP connections that are available.

5. What would be a reason for a computer user to use the Task Manager Performance tab?

- to increase the performance of the CPU
- **to check the CPU usage of the PC**
- to view the processes that are running and end a process if needed
- to view the services that are currently running on the PC

Explanation: The Performance tab is commonly used to check current computer performance. Two key areas that are shown are memory and CPU usage.

6. What are two advantages of the NTFS file system compared with FAT32? (Choose two.)

- **NTFS provides more security features.**
- NTFS allows faster formatting of drives.
- **NTFS supports larger files.**
- NTFS allows the automatic detection of bad sectors.

- NTFS is easier to configure.
- NTFS allows faster access to external peripherals such as a USB drive.

Explanation: The file system has no control over the speed of access or formatting of drives, and the ease of configuration is not file system-dependent.

7. Match the tabs of the Windows 10 Task Manager to their functions.

Explanation:

Details Allows for a process to have its affinity set.

Performance Displays resource utilization information for CPU, memory, network, disk, and others.

Startup Allows programs that are running on system startup to be disabled.

Services Allows for a start, stop or restart of a particular service.

8. Match the commonly used ports on a Linux server with the corresponding service.

Explanation:

25 SMTP

53 DNS

443 HTTPS

23 Telnet

9. Which two options are window managers for Linux? (Choose two.)

- **Gnome**
- Kali
- File Explorer
- **KDE**
- PenTesting

Explanation: The X Window System provides the basic framework for a GUI, but the GUI itself varies greatly between different distributions. Two window

managers are Gnome and KDE.

10. Which method can be used to harden a device?

- allow USB auto-detection
- **use SSH and disable the root account access over SSH**
- maintain use of the same passwords
- allow default services to remain enabled

Explanation: The basic best practices for device hardening are as follows:

Ensure physical security.

Minimize installed packages.

Disable unused services.

Use SSH and disable the root account login over SSH.

Keep the system updated.

Disable USB auto-detection.

Enforce strong passwords.

Force periodic password changes.

Keep users from re-using old passwords.

Review logs regularly.

11. What term describes a set of software tools designed to increase the privileges of a user or to grant access to the user to portions of the operating system that should not normally be allowed?

- package manager
- **rootkit**
- compiler
- penetration testing

Explanation: A rootkit is used by an attacker to secure a backdoor to a compromised computer, grant access to portions of the operating system normally not permitted, or increase the privileges of a user.

12. Why would a network administrator choose Linux as an

operating system in the Security Operations Center (SOC)?

- More network applications are created for this environment.
- It is more secure than other server operating systems.
- **The administrator has more control over the operating system.**
- It is easier to use than other operating systems.

Explanation: There are several reasons why Linux is a good choice for the SOC.

Linux is open source.

The command line interface is a very powerful environment.

The user has more control over the operating system.

Linux allows for better network communication control.

13. Match typical Linux log files to the function.

Explanation:

/var/log/secure used by RedHat and CentOS computers and tracks authentication-related events

/var/log/messages contains generic computer activity logs, and is used to store informational and noncritical system messages

/var/log/dmesg stores information related to hardware devices and their drivers

/var/log/auth.log used by Debian and Ubuntu computers and stores all authentication-related events

14. A client device has initiated a secure HTTP request to a web browser. Which well-known port address number is associated with the destination address?

- **443**
- 404
- 110
- 80

Explanation: Port numbers are used in TCP and UDP communications to

differentiate between the various services running on a device. The well-known port number used by HTTPs is port 443.

15. Consider the result of the ls -l command in the Linux output below. What are the file permissions assigned to the sales user for the analyst.txt file?

```
ls -l analyst.txt
```

```
-rwxrw-r-- sales staff 1028 May 28 15:50 analyst.txt
```

- write only
- read, write
- read only
- **read, write, execute**

Explanation: The file permissions are always displayed in the User, Group and Other order. In the example displayed, the file has the following permissions:

The dash (-) means that this is a file. For directories, the first dash would be replaced with a "d".

The first set of characters is for user permission (rwx). The user, sales, who owns the file can read, write and execute the file.

The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.

The third set of characters is for any other user or group permissions (r-). Any other user or group on the computer can only read the file.

16. A salesperson wants to embed the location on a digital photograph to record where it was taken. What technology, product, or setting allows this task to be accomplished?

- **geotagging**
- GPS
- RFID
- MIME

17. A user wants to synchronize some apps, movies, music, and ebooks between mobile devices. What are the two types of

connections used to synchronize this type of data? (Choose two.)

- Bluetooth
- **USB**
- **Wi-Fi**
- cellular
- NFC

18. Which cellular technology supports speeds up to 20 Gbps?

- **5G**
- 4G
- Zigbee
- Z-Wave

Explanation: Cellular technology standards are 1G, 2G, 3G, 4G, LTE, and 5G. 5G technology supports speeds up to 20 Gbps and is more efficient.

19. What are three reasons that users of iOS devices might use iCloud? (Choose three.)

- **to store documents and photos on remote servers**
- to provide access to the Apple App Store and the iTunes Store
- to enable automatic software updates and patches
- **to create an email account**
- **to make a backup copy of all of the data on their mobile device**
- to increase the security settings on their mobile device

Explanation: An Apple ID allows a user to create an iCloud email account. iCloud can be used to store personal documents, music, and photos. iCloud is also used for device synchronization and backup copies of personal data in case the mobile device is damaged or lost.

20. A traveling sales representative uses a cell phone to interact with the home office and customers, track samples, make sales calls, log mileage, and upload/download data while at a hotel. Which internet connectivity method would be a preferred method to use on the mobile device due to the low cost?

- DSL
- cable
- **Wi-Fi**
- cellular

Explanation: Mobile devices typically use either the cellular network or a Wi-Fi network to connect to the internet. The Wi-Fi connection is preferred because it uses less battery power and is free in many places.

21. Which protocol enables mail to be downloaded from an email server to a client and then deletes the email from the server?

- **POP3**
- IMAP
- HTTP
- SMTP

Explanation:

- With POP, mail is downloaded from the server to the client and then deleted on the server.
- SMTP is used for sending or forwarding email.
- Unlike POP, when a user connects via IMAP, copies of the messages are downloaded to the client application and the original messages are kept on the server until manually deleted.
- HTTP is used for web traffic data and is considered insecure.

22. What are two features of the Android operating system? (Choose two.)

- Each implementation of Android requires a royalty to be paid to Google.
- All available Android applications have been tested and approved by Google to run on the open source operating system.
- **Android has been implemented on devices such as cameras, smart TVs, and e-book readers.**
- **Android is open source and allows anyone to contribute to its development and evolution.**

- Android applications can only be downloaded from Google Play.

Explanation: As an open source operating system, Android allows anyone to contribute to the development and evolution of compatible software. Android has been implemented on a wide range of devices and platforms including cameras, smart TVs, and e-book readers. Royalties are not payable to Google, and Google has not tested and approved all available Android applications. Android applications are available from a range of sources.

23. What are two potential risks that could result from rooting or jailbreaking a mobile device? (Choose two.)

- enabling features that are disabled by a cellular carrier
- allowing the user interface to be extensively customized
- not properly creating or maintaining sandboxing features
- improving device performance
- enabling app access to the root directory

Explanation: Rooting and jailbreaking mobile devices allows customization of the OS which enables user and app access to the root directory. In addition, rooting and jailbreaking may cause a device to not properly create or maintain sandboxing features. Both of these can create security risks to the device. The three incorrect options are all considered potential benefits of rooting and jailbreaking mobile devices

24. What is required as an additional verification mechanism on iOS mobile devices when setting up biometric screen locks, such as Touch ID or Face ID?

- a linked email account
- a swipe code
- **a passcode**
- a pattern lock

Explanation: When setting up Touch ID and Face ID, you need to enter your passcode, or to create a passcode if one is not previously set up. The passcode will be used as an alternative manner to verify your identity.

25. Which statement describes the Touch ID in iOS devices?

- It is used to set the touch screen sensitivity.

- **It is the hash value of the user fingerprint.**
- It is the encryption key set by the user.
- It is used as the passcode.

Explanation: Apple uses a technology known as Touch ID in which the user sets up a template fingerprint scan that is converted into a unique hash and stored within a secure cache on the iOS device. The hash is used to authenticate with the user.

26. Which two tasks can be done with the iOS device Home button? (Choose two.)

- place apps into folders
- **return to the home screen**
- display the navigation icons
- respond to an alert
- **wake the device**

Explanation: The physical Home button on an iOS device can perform many functions depending on how it is used. Pressing the button while the device screen is turned off will wake the device. While an app is in use, pressing the Home button will return the user to the Home screen.

27. Android apps run primarily based on privileges enabled by the user. Sometimes an Android app requires extra privileges to access system components. How do Android apps run to accomplish both situations?

- Android apps run in a guest mode.
- Android apps run in a walled garden.
- **Android apps run in a sandbox.**
- Android apps run through a proxy service.

Explanation: Android apps run in a sandbox and have only the privileges enabled by the user. If an app needs to obtain permissions, a prompt will appear and the user can grant permissions through settings.

28. Which two location-specific services can the GPS feature on a mobile device offer? (Choose two.)

- planning a route between two locations
- displaying a map of a destination city while driving
- **delivering local advertising**
- playing local songs
- **displaying local weather information**

Explanation: GPS services allow app vendors and websites to know the location of a device and offer location-specific services such as local weather and advertising.

29. An employee wants to keep a local backup of iPhone data on a Windows laptop. What type of software does the employee need on the laptop to create this backup?

- **iTunes**
- Finder
- Google sync
- Time Machine

Explanation: Apple mobile devices can be backed up to a Windows PC or Laptop. iOS supports backups on iTunes running on a PC.

30. Which navigation icon on the system bar of an Android device is used to return to the previous screen?

- Recent Apps
- Menu
- **Back**
- Home

Explanation: The Back icon, if pressed, returns to the previous screen.

31. What is the outcome when a Linux administrator enters the man man command?

- The man man command configures the network interface with a manual address
- The man man command provides a list of commands available at the current prompt

- **The man man command provides documentation about the man command**
- The man man command opens the most recent log file

Explanation: The man command is short for manual and is used to obtain documentation about a Linux command. The command man man would provide documentation about how to use the manual.

32. Match the Linux command to the function.

Explanation: Place the options in the following order:

pwd displays the name of the current working directory

sudo runs a command as another user

chmod modifies file permissions

ps lists the processes that are currently running

33. What is the purpose of running mobile device apps in a sandbox?

- **to prevent malicious programs from infecting the device**
- to enable the phone to run multiple operating systems
- to bypass phone carrier restrictions that prevent access to unauthorized apps
- to enable separate app icons to be displayed on the home screen

Explanation: Mobile device apps are run in a sandbox that isolates them from other resources. Bypassing the phone carrier from preventing access to unauthorized apps is jailbreaking or rooting the device.

34. In the Linux shell, which character is used between two commands to instruct the shell to combine and execute these two commands in sequence?

- %
- \$
- #
- |

Explanation: In the Linux shell, several commands can be combined to perform a complex task. This technique is known as piping. The piping process is indicated by inserting the character “|” between two consecutive commands.